UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/785,407	02/25/2004	Govindarajan Krishnamurthi	60282.00168	8359

32294 7590 02/09/2007

SQUIRE, SANDERS & DEMPSEY L.L.P.
14TH FLOOR
8000 TOWERS CRESCENT
TYSONS CORNER, VA 22182

EXAMINER	
FARAGALLA, MICHAEL A	
ART UNIT	PAPER NUMBER
2617	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/785,407	KRISHNAMURTHI ET AL.	
	Examiner	Art Unit	
	Michael Faragalla	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-10 and 12-16* is/are rejected.

7)☒ Claim(s) *6 and 11* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims **2,8, and 13** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Consider **Claims 2,8, and 13,** the applicants invention is a method of reducing denial-of-service attacks by malicious mobile nodes. Claims 2,8, and 13 seem to be directed to a method of validating information of a mobile node after handover to a candidate access router.

Claim Rejections - 35 USC § 103

3. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a

later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims **1,3,7, and 12** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Frid et al (Patent number: 6,137,791)** in view of **Koodli et al (Patent number: 7,130,286).**

Consider **Claim 1**, Frid et al shows a method of reducing denial-of-service attacks by malicious mobile nodes in a mobile IP environment, said method comprising:

(a) Populating the cache with cache entries in response to actions initiated by mobile nodes (column 4, lines 36-48); (when a mobile travels into a geographical area, subscription data is stored regarding the mobile station).

(b) Each cache entry is tagged with an identity of an action initiating mobile node, which identity is based on information that is verifiable by the access routers and which cannot be modified arbitrarily by the mobile node (read to be the IP address of the mobile terminal) (column 5, lines 10-15).

(c) Wherein a total number of entries that can be tagged and thus introduced into a cache by any given node is limited (column 4, lines 36-48).

However, Frid et al does not specifically show that the method further comprising maintaining, by each of a plurality of access routers within the mobile IP environment, a cache of neighboring access routers as candidates and their associated access points.

In related art, Koodli et al shows that the method further comprising maintaining, by each of a plurality of access routers within the mobile IP environment, a cache of neighboring access routers as candidates and their associated access points (column 8, lines 22-27; column 7, lines 44-48); (for purposes of handover, a token is sent to the mobile terminal that includes information about the resources the mobile unit is eligible to access from the current access router, therefore, the router must keep information about the accessible resources).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Koodli et al into the

teaching of Frid et al in order to authorize mobile terminals to access the network (Koodli et al, abstract).

Consider **Claim 7,** Frid et al shows a system for reducing denial-of-service attacks by malicious mobile nodes in a mobile IP environment, said system comprising:

(a) A plurality of mobile nodes which are capable of populating the caches in response to actions initiated (column 4, lines 36-48); (when a mobile travels into a geographical area, subscription data is stored regarding the mobile station).

(b) Wherein the cache is configured such that each cache entry is tagged with an identity of the action initiating mobile node having thus created the entry, and that a total number of entries that can be tagged and thus introduced into the cache by any given node is limited (column 4, lines 36-48).

However, Frid et al does not specifically show that a plurality of access routers within the mobile IP environment, each router maintaining a cache of neighboring access routers as candidates and their associated access points.

In related art, Koodli et al shows that a plurality of access routers within the mobile IP environment, each router maintaining a cache of neighboring access routers as candidates and their associated access points (column 8, lines 22-27; column 7, lines 44-48); (for purposes of handover, a token is sent to the mobile terminal that includes information about the resources the mobile unit is eligible to access from the current access router, therefore, the router must keep information about the accessible resources).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Koodli et al into the teaching of Frid et al in order to authorize mobile terminals to access the network (Koodli et al, abstract).

Consider **Claim 12,** Frid et al shows an access router for reducing denial-of-service attacks by malicious mobile nodes in a mobile IP, said router comprising: A cache is arranged such that each cache entry is tagged with the identity of the mobile node having initiated the entry creation, and the total number of entries that can be tagged and thus introduced into the cache by any given node is limited (column 4, lines 36-48).

However, Frid et al does not specifically show that the router comprising a cache of neighboring access routers as candidates and their associated access points.

In related art, Koodli et al shows that the router comprising a cache of neighboring access routers as candidates and their associated access points (column 8, lines 22-27; column 7, lines 44-48); (for purposes of handover, a token is sent to the mobile terminal that includes information about the resources the mobile unit is eligible to access from the current access router, therefore, the router must keep information about the accessible resources).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Koodli et al into the teaching of Frid et al in order to authorize mobile terminals to access the network (Koodli et al, abstract).

Consider **Claim 3,** Frid et al in view of Koodli et al shows the method of claim 1, wherein the identity of the mobile node is an international mobile subscriber identity (IMSI) for cellular communication systems, and a network access identifier (NAI) for systems based on Internet Protocol (IP).

7. Claims **2,8, and 13** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Koodli et al (Patent number: US 7,130,286)** in view of **Norefors et al (Patent number: US 6,370,380).**

Consider **Claim 2,** Koodli et al shows a method of validating information of a mobile node within a candidate access router discovery procedure in a mobile IP environment, said method comprising:

(a) Generating a token by a first access router to which the mobile node was previously attached (column 8, lines 22-27); (the token is provide to the mobile node by the current access router).

(b) Sending the token from the access router to the mobile node within a message comprising a list of candidate access routers (column 7, lines 44-48).

(c) Sending the token from the mobile node to a second access router as selected candidate after a handover procedure between the first and second access routers (column 8, lines 22-27).

However, Koodli et al does not specifically show the step of sending the token within an exchange between the access routers specific to the discovery

procedure from the second access router back to the first access router for verification.

In related art, Norefors et al shows the step of sending the token within an exchange between the access routers specific to the discovery procedure from the second access router back to the first access router for verification (figure 3; column 3, 65-67; column 4, lines 1-6).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Norefors et al into the teaching of Koodli et al in order to for a mobile terminal to be protected during a handover (Norefors et al abstract).

Consider **Claim 8,** Koodli et al shows a system for validating information of a mobile node within a candidate access router discovery procedure in a mobile IP environment, comprising a first access router, said mobile node and a second access router, wherein:

(a) The first access router includes generating means for generating a token, first sending means for sending the token to the mobile node within a message comprising a list of candidate access routers (column 7, lines 44-48; column 8, lines 22-27); (the token is provide to the mobile node by the current access router).

(b) The mobile node includes second sending means for sending the token to the second access router as selected candidate after a handover procedure between the access routers (column 8, lines 22-27).

However, Koodli et al does not specifically show that the second access router includes third sending means for sending the token within an exchange between the access routers specific to the discovery procedure back to the first access router and verification means for verifying the token.

In related art, Norefors et al shows that the second access router includes third sending means for sending the token within an exchange between the access routers specific to the discovery procedure back to the first access router and verification means for verifying the token (figure 3; column 3, 65-67; column 4, lines 1-6).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Norefors et al into the teaching of Koodli et al in order to for a mobile terminal to be protected during a handover (Norefors et al abstract).

Consider **Claim 13,** Koodli et al shows an access router for validating information of a mobile node in a mobile IP, comprising:

(a) Generating means for generating a token (column 8, lines 22-27); (the token is provide to the mobile node by the current access router).

(b) First sending means for sending the token to the mobile node within a message comprising a list of candidate access routers (column 7, lines 44-48; column 8, lines 22-27); (the token is provide to the mobile node by the current access router).

However, Koodli et al does not specifically show that the access router further comprising second sending means for sending the token within an exchange within an exchange with another access router specific to the discovery procedure to the other access router; and verification means for verifying the token.

In related art, Norefors et al shows that the access router further comprising second sending means for sending the token within an exchange within an exchange with another access router specific to the discovery procedure to the other access router; and verification means for verifying the token (figure 3; column 3, 65-67; column 4, lines 1-6).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Norefors et al into the teaching of Koodli et al in order to for a mobile terminal to be protected during a handover (Norefors et al abstract).

8. Claims **4,5,9,10,14,15, and 16** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Frid et al (Patent number: 6,137,791)** in view of **Koodli et al (Patent number: 7,130,286)** and further in view of **Norefors et al (Patent number: US 6,370,380).**

Consider **Claim 4,** Frid et al as modified by Koodli et al shows the method according to claim 1, wherein an action initiated by a mobile node comprises a handover procedure of the mobile node between a previous access router and a

new access router, but fails to specifically show that said method further comprising:

Generating a token by the previous first access router; sending the token from the previous access router to the mobile node within a message comprising a list of candidate access routers; sending the token within a message specific to the discovery procedure from the mobile node to the new access router as selected candidate after the handover procedure.

In related art, Koodli et al shows that said method further comprising:

Generating a token by the previous first access router; sending the token from the previous access router to the mobile node within a message comprising a list of candidate access routers; sending the token within a message specific to the discovery procedure from the mobile node to the new access router as selected candidate after the handover procedure (column 7, lines 44-48; column 8, lines 22-27).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Koodli et al into the teaching of Frid et al in order to enable the mobile node to access network resources (Koodli et al; abstract).

However, the combination of Frid et al and Koodli et al does not disclose the step of sending the token within a neighbor exchange between the access routers resulting in cache entries being created or refreshed from the second access router back to the first router for verification.

In related art, Norefors et al shows the step of sending the token within a neighbor exchange between the access routers resulting in cache entries being created or refreshed from the second access router back to the first router for verification (figure 3; column 3, 65-67; column 4, lines 1-6).
Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Norefors et al into the teaching of Koodli et al in order to for a mobile terminal to be protected during a handover (Norefors et al abstract).

Consider **Claim 5,** Frid et al as modified by Koodli et al and as further modified by Norefors et al show the method according to claim 4, but fail to specifically show that the token is generated by maintaining by the previous access router a short list of random values used as keys to hash the identity of the mobile node, each key in the short list is associated with an integer index that is passed along with the token, and wherein upon receiving the token for verification, the previous access router uses the integer index to lookup the associated key, hash the identity of the mobile node sent in the neighbor exchange and compares the hash to the token.
However, in related art, Norefors et al shows that the token is generated by maintaining by the previous access router a short list of random values used as keys to hash the identity of the mobile node, each key in the short list is associated with an integer index that is passed along with the token, and wherein upon receiving the token for verification, the previous access router uses the

integer index to lookup the associated key, hash the identity of the mobile node sent in the neighbor exchange and compares the hash to the token (column 3, lines 46-67; figure 3).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Norefors into the teaching of Frid et al and Koodli et al in order to protect communications (Norefors et al, column 3, lines 63-65).

Consider **Claim 9,** Frid et al as modified by Koodli et al shows the system according to claim 7, but fails to specifically show that the access routers include generating means for generating a token, first sending means for sending the token to a mobile node within a message comprising a list of candidate access routers, the mobile nodes include third sending means for sending the token to a new access router as selected candidate after a handover procedure.

In related art Koodli et al shows that the access routers include generating means for generating a token, first sending means for sending the token to a mobile node within a message comprising a list of candidate access routers, the mobile nodes include third sending means for sending the token to a new access router as selected candidate after a handover procedure (column 7, lines 44-48; column 8, lines 22-27).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Koodli et al into the

teaching of Frid et al in order to enable the mobile node to access network resources (Koodli et al; abstract).

However, the combination of Frid et al and Koodli et al does not disclose that the system further comprising second means for sending the token within a neighbor exchange between access routers resulting in cache entries being created or refreshed, and verification means for verifying the token.

In related art, Norefors et al shows that the system further comprising second means for sending the token within a neighbor exchange between access routers resulting in cache entries being created or refreshed, and verification means for verifying the token (figure 3; column 3, 65-67; column 4, lines 1-6).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Norefors et al into the teaching of Koodli et al in order to for a mobile terminal to be protected during a handover (Norefors et al abstract).

Consider **Claim 10,** Frid et al as modified by Koodli et al and as further modified by Norefors et al shows the system according to claim 9, but fail to specifically show that the generating means include first hashing means for hashing the identity of the mobile node by using random values out of a short list as keys, associating means for associating each key in the list with an integer index, and wherein the verification means include a lookup table for the indices and their associated keys, second hashing means for hashing the identity of the mobile node and comparing means for comparing the hash to the token.

However, in related art, Norefors et al shows that the generating means include first hashing means for hashing the identity of the mobile node by using random values out of a short list as keys, associating means for associating each key in the list with an integer index, and wherein the verification means include a lookup table for the indices and their associated keys, second hashing means for hashing the identity of the mobile node and comparing means for comparing the hash to the token (column 3, lines 46-67; figure 3).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Norefors into the teaching of Frid et al and Koodli et al in order to protect communications (Norefors et al, column 3, lines 63-65).

Consider **Claim 14,** Frid et al as modified by Koodli et al shows the access router according to claim 12, but fails to specifically show that the access router further comprising:

Generating means for generating a token, first generating means for sending the token to a mobile node within a message comprising a list of candidate access routers.

In related art, Koodli et al shows that the access router further comprising:

Generating means for generating a token, first generating means for sending the token to a mobile node within a message comprising a list of candidate access routers (column 7, lines 44-48; column 8, lines 22-27).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Koodli et al into the teaching of Frid et al in order to enable the mobile node to access network resources (Koodli et al; abstract).

However, the combination of Frid et al and Koodli et al does not disclose that the access router further comprising second sending means for sending the token within a neighbor exchange with another access router resulting in cache entries being created or refreshed, and verifying the token.

In related art, Norefors et al shows that the access router further comprising second sending means for sending the token within a neighbor exchange with another access router resulting in cache entries being created or refreshed, and verifying the token (figure 3; column 3, 65-67; column 4, lines 1-6).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Norefors et al into the teaching of Koodli et al in order to for a mobile terminal to be protected during a handover (Norefors et al abstract).

Consider **Claim 15,** Frid et al as modified by Koodli et al and as further modified by Norefors et al shows the access router according to claim 14, but fail to specifically show that the generating means include first hashing means for hashing the identity of the mobile node by using random values out of a short list as keys, associating means for associating each key in the list with an integer index, and the verification means include a lookup table for the indices and their

associated keys, second hashing for hashing the identity of the mobile node and comparing means for comparing the hash to the token.

However, in related art, Norefors et al shows that the generating means include first hashing means for hashing the identity of the mobile node by using random values out of a short list as keys, associating means for associating each key in the list with an integer index, and the verification means include a lookup table for the indices and their associated keys, second hashing for hashing the identity of the mobile node and comparing means for comparing the hash to the token (column 3, lines 46-67; figure 3).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Norefors into the teaching of Frid et al and Koodli et al in order to protect communications (Norefors et al, column 3, lines 63-65).

Consider **Claim 16,** Frid et al as modified by Koodli et al and as further modified by Norefors et al shows the access router according to claim 15, but fail to specifically show that the generating means are configured to generate new keys with progressing time, to add them to the head of the list and remove old keys.

However, in related art, Norefors et al shows that the generating means are configured to generate new keys with progressing time, to add them to the head of the list and remove old keys (column 3, lines 60-67).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Norefors into the teaching

of Frid et al and Koodli et al in order to protect communications (Norefors et al, column 3, lines 63-65).

Allowable Subject Matter

9. Claims **6 and 11** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

(1) CONTEXT TRANSFER SYSTEMS AND METHODS IN SUPPORT OF MOBILITY **(Patent number: US 7,050,793).**

(2) METHOD AND ARRANGEMENT IN A TELECOMMUNICATION SYSTEM **(Patent number: 6,553,231).**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Faragalla whose telephone number is (571) 270-1107. The examiner can normally be reached on Mon-Fri 7:30 am-5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nick Corsaro can be reached on (571) 272-7876. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Michael Faragalla

01/27/2007

EDAN ORGAD
PRIMARY PATENT EXAMINER